

Noncanonical number systems in the integers

Christiaan van de Woestijne

Institut für Mathematik B, Technische Universität Graz, 8010 Graz, Austria

Abstract

The well known binary and decimal representations of the integers, and other similar number systems, admit many generalisations. Here, we investigate whether still every integer could have a finite expansion on a given integer base b , when we choose a digit set that does not contain 0. We prove that such digit sets exist and we provide infinitely many examples for every base b with $|b| \geq 4$, and for $b = -2$. For the special case $b = -2$, we give a full characterisation of all valid digit sets.

Key words: Radix systems

1 Introduction and results

A *number system* is a coherent notation system for numbers. There are many possibilities to define such systems, but in this paper we will consider only generalisations of the *positional* number systems, like the binary and decimal notations. In such systems, one represents numbers by finite expansions of the form

$$a = \sum_{i=0}^{\ell} d_i b^i, \quad (1.1)$$

where the d_i are taken from a finite set of digits, and b is the *base* of the system. For example, taking for b an integer greater than 1 and using digits $\{0, 1, \dots, b-1\}$, we can represent all nonnegative integers in the form (1.1), and these representations are in fact unique. However, if we want to represent *all integers* in this form, we must change either the base or the digit set; for example, we can take an integer base b with $b \leq -2$, and digits $\{0, 1, \dots, |b|-1\}$, as proved already by Grünwald in 1885 [1].

In this paper, we will restrict ourselves to number systems within the set of integers. The basic definitions are then as follows.

Definition 1.1 *A pre-number system in the ring of integers \mathbb{Z} is given by an integer b and a finite set of integers \mathcal{D} satisfying the following properties:*

- (i) we have $|b| \geq 2$;
- (ii) the elements of \mathcal{D} cover all the cosets of integers modulo b .

The integer b is called the *base of the pre-number system*, and \mathcal{D} is the *digit set*. If $|\mathcal{D}| = |b|$, we say that \mathcal{D} is *irredundant*, otherwise it is *redundant*. In an irredundant digit set, the unique digit that represents the coset of 0 is called the *zero digit*.

A *pre-number system* $(\mathbb{Z}, b, \mathcal{D})$ is a number system if every $a \in \mathbb{Z}$ has a finite expansion of the form

$$a = \sum_{i=0}^{\ell-1} d_i b^i$$

where all d_i are in \mathcal{D} and where ℓ is a positive integer.

If $(\mathbb{Z}, b, \mathcal{D})$ is a number system, we call \mathcal{D} a *valid digit set* for b .

The notation $(\mathbb{Z}, b, \mathcal{D})$ for a pre-number system in \mathbb{Z} is motivated by the fact that pre-number systems may be defined in much more general rings and other sets (see the forthcoming paper [2]), where instead of \mathbb{Z} we indicate the set of numbers, or number-like elements, that we want to have a finite representation. In the present paper, however, all pre-number systems will be in \mathbb{Z} .

Many generalisations of this definition are possible. Already Knuth [3, Section 4.1] gave many interesting variants. For all variants where the basis remains integral in some sense, such as an algebraic integer or an integer matrix, we would like to refer to Section 3 of the survey paper [4]. It is possible to consider nonintegral bases; this was done in [5], [6, Section 5.3.3], and [7]. One could take a positive b and nonnegative digits, and look only at the property of representing all *nonnegative* integers in the form (1.1); here, a complete classification of all possible digit sets (which must contain 0) was achieved in [8], and generalisations to the higher-dimensional case are given in [9] and [10]. There are interesting number systems that use redundant digit sets, such as those discussed in [11,12]; in the guise of addition chains, several such systems are useful for speeding up operations in elliptic curve cryptosystems (see [13, Chapter 9]).

Virtually all papers dealing with number systems as defined above, or with their generalisations, have used the additional requirement that 0 be in the digit set. The main goal of this paper is to explore the consequences when we drop this restriction, while remaining within the framework of Definition 1.1. We will discuss higher-dimensional generalisations in another paper [2]. Number systems without zero in the case where the base b is a power of ± 2 were proposed by Möller for the purpose of avoiding Side Channel Attacks in elliptic curve cryptography (see [14, Section 4.4] and [13, Section 29.1.1.a]).

The basic implications of Definition 1.1 will be discussed in Section 2. For example, if 0 is not a digit, we cannot pad expansions with zeros if we want

to make them longer; we will be forced to use repetitions of some sequence of nonzero digits that nonetheless has zero value. We will show that such a sequence always exists, whenever we have a *number system*. We also show that the length of such sequences goes to ∞ with the size of the *zero digit*. Next, we construct a few basic examples of digit sets with without 0 for any base b . Finally, we show that a valid digit set cannot be translated over an arbitrarily large integer without losing the number system property, even if it contains 0 and we leave the 0 in place.

In Section 3, we will prove the existence of infinitely many distinct sets of nonzero digits in \mathbb{Z} for any integer base b with $|b| \geq 4$, the main results being Theorems 3.7 and 3.14. This complements known results for digit sets that do have 0, which have been obtained by Matula [15] and Kovács and Pethő [16].

As for bases with $|b| \leq 3$, we have a pre-number system if $b = \pm 2$ or $b = \pm 3$. Now for $b = 2$, no digit set at all will yield a number system, whether including 0 or not; see Corollary 2.5 for a proof. For $b = -2$, in Section 4 we will characterise *all* possible digit sets that yield a number system in \mathbb{Z} ; although infinite in number, it will turn out that their structure is different from the infinite families obtained for larger bases in Section 3. The main result is Theorem 4.1. For $|b| = 3$, we have been unable to obtain the existence of infinitely many digit sets without zero, which therefore remains an open problem.

2 Digit sets with and without zero

We will now explore the consequences of not having 0 as a digit in a number system. First, we extend some well known results and definitions to the more general context defined above; see [4, Sections 2.1, 2.2, 3.1, and 3.2] and references therein for more background on these notions.

2.1 Notations and extensions

Let $(\mathbb{Z}, b, \mathcal{D})$ be a pre-number system. For the rest of the paper, we will assume that all digit sets are *irredundant*. It follows that, given $a \in \mathbb{Z}$, there exists a unique digit $d_a \in \mathcal{D}$ such that $a - d_a$ is divisible by b .

In particular, there will be a unique digit that is itself divisible by b ; this is the digit corresponding to the integer 0, and, as in Definition 1.1, we will call it the *zero digit*, whether it be equal to 0 or not.

Definition 2.1 Given a pre-number system $(\mathbb{Z}, d, \mathcal{D})$, define maps

$$\begin{aligned} d : \mathbb{Z} &\rightarrow \mathcal{D} : a \mapsto d \in \mathcal{D} \text{ such that } b \text{ divides } a - d; \\ T : \mathbb{Z} &\rightarrow \mathbb{Z} : a \mapsto (a - d(a))/b. \end{aligned} \tag{2.1}$$

The map T is called the *dynamic mapping* of $(\mathbb{Z}, b, \mathcal{D})$. The name obviously comes from dynamical system theory; this connection is given in more detail in [17]. The *digit function* d can also be viewed as a redefinition of the usual modulo operator: we could say that $d(a)$ is a modulo b , with respect to the digits \mathcal{D} .

We will sometimes use the notation $a \rightarrow a'$ whenever we have $T(a) = a'$.

Theorem 2.2 A pre-number system $(\mathbb{Z}, b, \mathcal{D})$, with dynamic mapping T , is a number system if and only if, for all $a \in \mathbb{Z}$, we have $T^i(a) = 0$ for some $i \geq 1$.

Proof. For any $a \in \mathbb{Z}$, we want to find the expansion

$$a = \sum_{i=0}^{\ell-1} d_i b^i \tag{2.2}$$

with digits in \mathcal{D} and $\ell \geq 1$. Now the proof is easily done by induction on ℓ . \square

The considerations just given show that whether a given pre-number system has the number system property depends on the structure of the *discrete dynamical system* on \mathbb{Z} given by the map T .

The characterisation given in Theorem 2.2 can be made into a finite algorithm for deciding the number system property, because the dynamical system just defined is contractive and therefore has a finite *attractor set* \mathcal{A} [17]. The set \mathcal{A} by definition has the property that for all $a \in \mathbb{Z}$, we have $T^n(a) \in \mathcal{A}$ for n sufficiently large, and also that $a \in \mathcal{A}$ implies $T(a) \in \mathcal{A}$.

Now because the attractor \mathcal{A} is a finite set, the sequence $(T^i(a))_{i \geq 0}$ must be purely periodic for any $a \in \mathcal{A}$; the elements of \mathcal{A} that constitute one full period are called a *cycle* in \mathcal{A} . In the notation given at the beginning of the section, we can write a cycle in \mathcal{A} as

$$a_0 \rightarrow a_1 \rightarrow \dots \rightarrow a_n = a_0,$$

where $a_{i+1} = T(a_i)$ for all i .

The following Theorem is the extension, to general digit sets, of the usual formulation that in a number system the attractor should contain just the element 0 (given as Theorem 3 in [16]).

Theorem 2.3 *The pre-number system $(\mathbb{Z}, b, \mathcal{D})$ is a number system if and only if the attractor \mathcal{A} consists of exactly one cycle under the map T , and this cycle contains 0.*

Proof. We have seen that $a \in \mathbb{Z}$ has a finite expansion if and only if $T^i(a) = 0$ for some $i \geq 1$. Now if $0 \notin \mathcal{A}$ and $a \in \mathcal{A}$, then $T^i(a) \neq 0$ for all $i \geq 0$, so that a cannot have a finite expansion, and if a is contained in some cycle in \mathcal{A} that does not pass through 0, we also have $T^i(a) \neq 0$ for all i .

Conversely, if $a \in \mathbb{Z}$, then $T^n(a) \in \mathcal{A}$ whenever n is large enough. Thus if the attractor has just one cycle that also contains 0, there must exist some $i \geq 1$ with $T^i(a) = 0$, as desired. \square

The Theorem in particular disallows 1-cycles in the attractor other than $0 \rightarrow 0$. The next Lemma gives a well-known characterisation of such cycles, to be used later.

Lemma 2.4 *Let $(\mathbb{Z}, b, \mathcal{D})$ be a pre-number system, with attractor \mathcal{A} . Then \mathcal{A} contains a 1-cycle $a \rightarrow a$ for some $a \in \mathbb{Z}$ if and only if $(1 - b)a$ is an element of the digit set \mathcal{D} .*

Proof. Let $d \in \mathcal{D}$, and suppose $d = (1 - b)a$ for some $a \in \mathbb{Z}$. It follows that

$$T(a) = (a - d)/b = a,$$

so that \mathcal{A} has the 1-cycle $a \rightarrow a$. Conversely, if $a \rightarrow a$, then by definition

$$a = T(a) = (a - d)/b,$$

so we find $d = (1 - b)a$. \square

Corollary 2.5 *Let $(\mathbb{Z}, b, \mathcal{D})$ be a number system. Then \mathcal{D} contains no nonzero multiples of $1 - b$. A fortiori, $|1 - b| \neq 1$.*

Proof. Suppose $d = (1 - b)a$ for some $a \in \mathbb{Z}$, where $d \in \mathcal{D}$ is nonzero. Then by Lemma 2.4,

$$a \rightarrow a$$

is a nontrivial 1-cycle in the attractor \mathcal{A} , which contradicts Theorem 2.3. Furthermore, if $1 - b$ is a unit in \mathbb{Z} , then obviously all digits are multiples of $1 - b$, which contradicts the first claim. \square

We are naturally interested in *bounding the size* of the attractor. The first bound that we will use is well known, and we leave the proof to the reader.

Lemma 2.6 *Let $(\mathbb{Z}, b, \mathcal{D})$ be a pre-number system with dynamic mapping T , let $K = \max_{d \in \mathcal{D}} |d|$, and let $L = K/(|b| - 1)$. Let $a \in \mathbb{Z}$.*

- (i) *If $|a| > L$, then $|T(a)| < |a|$.*
- (ii) *If $|a| \leq L$, then also $|T(a)| \leq L$.*

Lemma 2.6 of course implies that $|a| \leq L$ for all $a \in \mathcal{A}$; however, for pre-number systems in the integers, we can do better than this. The bounds in Theorem 2.9 below are due to D. Matula [15, Lemma 6] for the case where $0 \in \mathcal{D}$. For the general case, Matula's argument breaks down, so we will reprove the result. We will use the following definition, which is interesting in its own right.

Definition 2.7 *Let $(\mathbb{Z}, b, \mathcal{D})$ be a pre-number system and n a positive integer. We define the n -fold digit set as*

$$\mathcal{D}^n = \left\{ \sum_{i=0}^{n-1} d_i b^i \mid d_i \in \mathcal{D} \right\}$$

and the n -fold pre-number system as $(\mathbb{Z}, b^n, \mathcal{D}^n)$.

Note that \mathcal{D}^n is a complete system of representatives of \mathbb{Z} modulo b^n if and only if \mathcal{D} is such a system modulo b . It follows that the n -fold pre-number system is well defined. The next result gives some properties of such systems.

Proposition 2.8 *Let $(\mathbb{Z}, b, \mathcal{D})$ be a pre-number system with dynamic mapping T and attractor \mathcal{A} , and let n be a positive integer. Then:*

- (i) *The dynamic mapping of $(\mathbb{Z}, b^n, \mathcal{D}^n)$ is equal to T^n .*
- (ii) *The attractor of $(\mathbb{Z}, b^n, \mathcal{D}^n)$ is equal to \mathcal{A} .*
- (iii) *$(\mathbb{Z}, b^n, \mathcal{D}^n)$ is a number system if and only if $(\mathbb{Z}, b, \mathcal{D})$ is a number system and $\gcd(n, |\mathcal{A}|) = 1$.*

Proof. Let \tilde{T} be the dynamic mapping of $(\mathbb{Z}, b^n, \mathcal{D}^n)$. For all $a \in \mathbb{Z}$, we have

$$\tilde{T}(a) = \frac{a - \sum_{i=0}^{n-1} d_i b^i}{b^n},$$

where the digits $d_0, \dots, d_{n-1} \in \mathcal{D}$ are chosen so as to make the numerator divisible by b^n . Thus clearly \tilde{T} is equal to the n -fold composition of T with itself, as claimed.

Now let $a \in \mathbb{Z}$ be periodic under T with period length ℓ ; then a is periodic under T^n with period length $\text{lcm}(n, \ell)/n = \ell/\gcd(n, \ell)$. Conversely, if a is

periodic under T^n with period length ℓ , then a is also periodic under T , with some period length that divides $n \cdot \ell$. This proves (ii).

Part (iii) is an easy consequence of (i), together with Theorem 2.3; one notes that a cycle of length ℓ in \mathcal{A} is broken up into pieces of length $\ell / \gcd(n, \ell)$ if we replace T by T^n . \square

Examples. Theorem 4.1 implies that $\{1, 2\}$ is a valid digit set for the base -2 . The n -fold digit set \mathcal{D}^n is equal to $\{-2^n + 1, \dots, -1, 0\}$ if n is even and to $\{1, 2, \dots, 2^n\}$ if n is odd. The Proposition now tells us that \mathcal{D}^n is valid for base $(-2)^n$ precisely for odd n . In fact, the attractor for all n is equal to $\{0, 1\}$, but for even n the 2-cycle $0 \rightarrow 1 \rightarrow 0$ is broken up into two 1-cycles, and the criterion of Theorem 2.3 is violated. One could also have used the obvious criterion that any valid digit set for a positive base must contain both negative and positive digits.

When the starting digit set \mathcal{D} contains 0, the attractor \mathcal{A} is just $\{0\}$, and the condition on the gcd in (iii) is trivially satisfied. Thus, when $0 \in \mathcal{D}$, $(\mathbb{Z}, b, \mathcal{D})$ is a number system if and only if all its n -fold pre-number systems are number systems; this is Lemma 4 in [15].

Theorem 2.9 *Let $(\mathbb{Z}, b, \mathcal{D})$ be a pre-number system with attractor \mathcal{A} , and let $d = \min_{d \in \mathcal{D}} d$ and $D = \max_{d \in \mathcal{D}} d$. Then for all $a \in \mathcal{A}$, we have*

$$\begin{aligned} \frac{-D}{b-1} &\leq a \leq \frac{-d}{b-1} && \text{if } b > 0; \\ \frac{-db-D}{b^2-1} &\leq a \leq \frac{-Db-d}{b^2-1} && \text{if } b < 0. \end{aligned}$$

Proof. The proof when $b > 0$ is easy and is left to the reader. For the case $b < 0$, we use the 2-fold pre-number system $(\mathbb{Z}, b^2, \mathcal{D}^2)$, which by Proposition 2.8 has the same attractor as $(\mathbb{Z}, b, \mathcal{D})$, but with the positive base b^2 . Furthermore, the largest digit of \mathcal{D}^2 is given by $kb + K$ and the smallest by $Kb + k$, because b is negative. Thus, we are reduced to the case of a positive base. \square

Remark. The interval $[-L, L]$ of Lemma 2.6 has the property that $|a| \leq L$ implies $|T(a)| \leq L$; we will use this property in Lemma 2.17 below. The intervals in Theorem 2.9 only have this property for $b > 0$. If I denotes the interval given in Theorem 2.9 for a negative b , then $a \in I$ does imply $T^2(a) \in I$, but we may have $T(a) \notin I$.

2.2 Zero expansions

If, in any number system, we have a digit 0 at our disposal, it is clear that we can extend any finite expansion for a to any length that we like, by putting zeros in front. We now prove an analogous property for a number system with any given digit set, although we will need repeated instances of a sequence of more than one digit long to obtain the same effect as zero padding.

Definition 2.10 *A zero expansion of a pre-number system $(\mathbb{Z}, b, \mathcal{D})$ is a sequence of digits $(d_0, \dots, d_{\ell-1})$ in \mathcal{D} , with $\ell \geq 1$, such that*

$$\sum_{i=0}^{\ell-1} d_i b^i = 0. \quad (2.3)$$

Note that a zero expansion is already determined by its length; in particular, if a pre-number system has a zero expansion at all, then it also has a *shortest* zero expansion, which is uniquely determined.

Theorem 2.11 *Every number system $(\mathbb{Z}, b, \mathcal{D})$ has a unique zero expansion of minimal length.*

Proof. We use Theorem 2.3; thus, let $0, T(0), T^2(0), \dots, T^n(0)$ be the elements of the attractor \mathcal{A} , where we have $T^{n+1}(0) = 0$. The result follows immediately, using the same argument as in the proof of Lemma 2.2. \square

Examples. We give some examples of zero expansions, which we write starting from the least significant digit.

- (i) If $0 \in \mathcal{D}$, the zero expansion is simply (0) .
- (ii) Take a base $b \in \mathbb{Z}$, with $|b| \geq 2$, and take digits $\{1, 2, \dots, |b|\}$. Obviously, the zero digit here is $|b|$. In this case, we have a zero expansion if and only if $b < 0$. Indeed, if $b < 0$, the zero expansion is given by $(|b|, 1)$, because

$$|b| \cdot b^0 + 1 \cdot b^1 = 0.$$

If $b > 0$, we cannot have a zero expansion: we have $d(0) = b$, so $T(0) = (0 - b)/b = -1$, but negative numbers cannot be represented by nonnegative digits on a positive base. Indeed, we have $T(-1) = \frac{-1 - (b-1)}{b} = -1$, so the zero expansion would be the infinite sequence $(b, b-1, b-1, b-1, \dots)$. This implies immediately that

$$(\mathbb{Z}, b, \{1, \dots, |b|\})$$

for $b > 0$ cannot be a number system.

- (iii) If $b \geq 2$, and we take the digits $\{-1, 1, 2, \dots, b-2, b\}$, then we have the zero expansion $(b, -1)$. Note that this digit set gives a number system for any b , by Theorem 2.13.
- (iv) We will show in Theorem 2.12 that the length of the zero expansion increases with the size of the zero digit. As an example of this behaviour, let $b = -2$, choose an integer $i \geq 0$, and let $\mathcal{D} = \{1, 3^i + 1\}$; by Theorem 4.1 below, this always gives a number system. The zero digit here is the even number $3^i + 1$; it follows from Lemma 4.2 that the zero expansion has length 3^i .

For a general digit set, the length of the zero expansion becomes an important parameter in many kinds of number system constructions. For example, if we want to pad an expansion to obtain some exact length ℓ , we must know that the length to be padded is divisible by the length of the zero expansion. This problem will occur in the proof that there are infinitely many digit sets not containing zero, for any base $b \in \mathbb{Z}$ (Theorems 3.7 and 3.14 below).

The last result in this subsection shows that in general, the length of the zero expansion grows to infinity with the size of the zero digit.

Theorem 2.12 *Let $(\mathbb{Z}, b, \mathcal{D})$ be a pre-number system with $0 \in \mathcal{D}$. Then for each $\ell \geq 1$, there are only finitely many $d \in b\mathbb{Z}$ such that the pre-number system $(\mathbb{Z}, b, \mathcal{D} \setminus \{0\} \cup \{d\})$ has a zero expansion of length ℓ .*

Proof. Let $\ell \geq 1$, let $d \in b\mathbb{Z}$, and let $(d_0, d_1, \dots, d_{\ell-1})$ be the zero expansion of $(\mathbb{Z}, b, \mathcal{D} \setminus \{0\} \cup \{d\})$, as defined by (2.3). Let I be the set of those i in $\{0, \dots, \ell-1\}$ for which $d_i = d$; note that $0 \in I$, because $d_0 = d$. From $\sum_{i=0}^{\ell-1} d_i b^i = 0$, we then obtain

$$\left(\sum_{i \in I} b^i \right) d = - \sum_{i \notin I} b^i d_i. \quad (2.4)$$

The element on the left is nonzero, because $|b| \geq 2$, and hence a sum of distinct powers of b cannot be 0.

Now we finish the proof of the Theorem. The right hand side of (2.4) clearly takes at most $(|b| - 1)^{\ell-1}$ distinct values. To each of these values corresponds at most one value for d . This completes the proof. \square

2.3 The first digit sets

Note that the base $b = 2$, although it can be used to define pre-number systems, must be excluded. In fact, $b - 1 = 1$ in this case, and Corollary 2.5 then tells us that there exists no digit set $\{d_0, d_1\}$ in \mathbb{Z} such that $(\mathbb{Z}, 2, \{d_0, d_1\})$

is a number system. For example, the well-known binary digits $\{0, 1\}$ can only represent nonnegative integers on base 2.

The restriction to just 2 digits is important here: for example, one can show that every integer has a unique Non-Adjacent Form (NAF) expansion on base 2 with the digits $\{0, 1, -1\}$ (see [18]). In formulae: every $a \in \mathbb{Z}$ can be written uniquely in the form

$$a = \sum_{i=0}^{\ell} d_i 2^i, \quad d_i \in \{0, \pm 1\}, d_i d_{i+1} = 0.$$

In this paper, however, we only consider irredundant digit sets, hence only digit sets of cardinality $|b|$ if the base is b . Our first result here, which is new as far as digit sets without zero are concerned, is as follows.

Theorem 2.13 *Let $b \in \mathbb{Z}$, with $|b| \geq 3$. Let \mathcal{D} be a complete residue system modulo b , such that*

- (i) $|d| \leq |b|$ for all $d \in \mathcal{D}$;
- (ii) either $1 \in \mathcal{D}$ or $-1 \in \mathcal{D}$;
- (iii) neither $b-1 \in \mathcal{D}$ nor $-b+1 \in \mathcal{D}$.

Then $(\mathbb{Z}, b, \mathcal{D})$ is a number system.

Proof. Define $T : \mathbb{Z} \rightarrow \mathbb{Z}$ as in Definition 2.1; by Theorem 2.2, we must prove that for all $a \in \mathbb{Z}$, there exists $n \geq 1$ such that $T^n(a) = 0$. By the Lemma, it is enough to do this for all a with $|a| \leq 2$, as $|k| \leq |b|$ and $|K| \leq |b|$ in our case.

For any b , if $|a| = 1$, we easily verify that either $Ta = 0$ or $T^2a = 0$, using the second and third assumptions. If $a = 2$, then either 2 or $-|b| + 2$ is a digit, so that $T(2) \in \{0, 1, -1\}$, and the same holds for $a = -2$.

We see that for all nonzero $a \in \mathbb{Z}$, we have $T^n a = 0$ for some n . This immediately also shows the existence of a zero cycle, because if $a = T(0)$, there exists $n \geq 0$ such that $T^n a = 0$, so that $T^{n+1}(0) = 0$. \square

Remarks. Note that the proof actually allows to relax condition (i) to $|d| \leq 2|b| - 2$.

The above result does not hold as stated for base -2 . Base -2 is actually a quite special case, which will be worked out completely in Section 4.

The assumptions about the presence of ± 1 in \mathcal{D} are necessary. The only representatives of ± 1 that are allowed are ± 1 themselves, $b \pm 1$, and $-b \pm 1$. If

$b-1$ or $-b+1$ are digits, then we get a nonzero 1-cycle by Lemma 2.4. If both $b+1$ and $-b-1$ are in \mathcal{D} , we see

$$T(1) = \frac{1 - (b+1)}{b} = -1, \quad T(-1) = \frac{-1 - (-b-1)}{b} = 1,$$

which also gives a non-zero cycle.

Example. A nice example of a digit set without zero that always works, is given by the *odd digit set*.

Definition 2.14 For an odd $b \in \mathbb{Z}$, define the set of odd digits modulo b as

$$\mathcal{D}_{b,\text{odd}} = \begin{cases} \{-b+2, -b+4, \dots, -1, 1, \dots, b-2, b\} & \text{if } b > 0; \\ \{b, b+2, \dots, -1, 1, \dots, -b-2\} & \text{if } b < 0. \end{cases}$$

Corollary 2.15 Let $b \in \mathbb{Z}$ be odd, with $|b| \geq 3$. Then $(\mathbb{Z}, b, \mathcal{D}_{b,\text{odd}})$ is a number system.

Proof. The only thing to show, before we can apply the Theorem, is that $\mathcal{D}_{b,\text{odd}}$ contains a complete system of representatives modulo b . Now if $d \in \mathcal{D}_{b,\text{odd}}$ is negative, then $d+b$ is even and between 0 and $b-1$. Thus the classes of $\{0, \dots, b-1\}$ or $\{1, \dots, b\}$ are all represented in $\mathcal{D}_{b,\text{odd}}$. \square

2.4 Translation of digit sets

In the quest for classification of all valid digit sets, now that we know that having 0 as a digit is not essential, we might think that one valid digit set could give rise to infinitely many digit sets by simple translation. Below, we show (Theorem 2.18) that translation of the digit set over a fixed integer will destroy the number system property if the integer is too large. In fact, we prove that when $0 \in \mathcal{D}$, the same holds if we translate all nonzero digits, while leaving 0 in place.

We begin with a basic observation.

Lemma 2.16 Let $(\mathbb{Z}, b, \mathcal{D})$ be a pre-number system, with attractor \mathcal{A} . If $(\mathbb{Z}, b, \mathcal{D})$ is a number system, then \mathcal{A} contains at least one element of \mathcal{D} .

Proof. Consider the zero cycle

$$0 \rightarrow a_1 \rightarrow \dots \rightarrow a_\ell \rightarrow 0,$$

where $a_1, \dots, a_\ell \in \mathcal{A}$. If $a_\ell \rightarrow 0$, that means that the digit representing the coset of a_ℓ is equal to a_ℓ , in other words, that $a_\ell \in \mathcal{D}$. \square

The elements of the attractor may be thought of as “small”, at least when compared the the largest digit; therefore, the previous lemma tells us that at least one digit is “small”. However, we want to strengthen the claim of the lemma to say that at least one *nonzero* digit must be small. Note that when $0 \in \mathcal{D}$, the number system property is equivalent to $\mathcal{A} = \{0\}$, so this nonzero digit cannot be an element of the attractor. The next result, which generalises Theorem 4 from [16], shows that next to the attractor also the set $\{a \in \mathbb{Z} \mid |a| \leq L\}$ from Lemma 2.6 has some importance.

Lemma 2.17 *Let $(\mathbb{Z}, b, \mathcal{D})$ be a number system, and let K and L be as in Lemma 2.6. If K is large enough, then there is at least one $d \in \mathcal{D}$, with $d \neq 0$, such that*

$$|d| \leq L.$$

Proof. Let $a_0 \in \mathbb{Z}$ have $a_0 \neq 0$ and $|a_0| \leq L$; we may assume that K is so large that $L \geq 1$. By our assumption, a_0 has a finite expansion on the base b with digits in \mathcal{D} . Thus, there exist a minimal ℓ and $a_i \in \mathbb{Z}$ with

$$a_0 \rightarrow T(a_0) = a_1 \rightarrow \dots \rightarrow a_\ell \rightarrow 0.$$

By Lemma 2.6, we know that $|a_i| \leq L$ for all i . On the other hand, a_ℓ must be a digit, and by the minimality of ℓ we know that $a_\ell \neq 0$. \square

Theorem 2.18 *Let $(\mathbb{Z}, b, \mathcal{D})$ be a pre-number system with $|b| \geq 3$, and for $t \in \mathbb{Z}$, define \mathcal{D}_t as $\{d + t \mid d \in \mathcal{D}\}$. Then there are only finitely many $t \in \mathbb{Z}$ such that $(\mathbb{Z}, b, \mathcal{D}_t)$ is a number system.*

If $0 \in \mathcal{D}$, then the same statement holds for $\tilde{\mathcal{D}}_t = \{d + t \mid d \in \mathcal{D}, d \neq 0\} \cup \{0\}$.

Proof. Let $K_t = \max_{d \in \mathcal{D}_t} |d|$; by Lemma 2.6, we see that

$$|a| \leq K_t / (|b| - 1) \tag{2.5}$$

for all a in the attractor \mathcal{A}_t of $(\mathbb{Z}, b, \mathcal{D}_t)$. In particular, by Lemma 2.16, this inequality holds for at least one digit in \mathcal{D}_t ; note that $1/(|b| - 1) < 1$ by our assumptions. But as $|t| \rightarrow \infty$, clearly $\frac{|d|}{K_t} \rightarrow 1$ for all $d \in \mathcal{D}_t$, so that (2.5) is violated for all $d \in \mathcal{D}_t$ when $|t|$ is sufficiently large. This is a contradiction, and the first claim is proved.

For the second claim, we use Lemma 2.17 to show that, when t is large enough, we must have $|d| \leq K_t / (|b| - 1)$ for some nonzero $d \in \tilde{\mathcal{D}}_t$. The rest of the argument is the same. \square

Remark. The argument of the proof makes essential use of the inequality $1/(|b| - 1) < 1$, and therefore the proof breaks down when $|b| = 2$. In fact, we will obtain the assertions of the Theorem for the case $|b| = 2$ below, using a specialised argument.

3 Infinitely many digit sets

Having established the existence of good digit sets with and without zero for any integer base b with $|b| \geq 2$ (except $b = 2$) in Theorem 2.13, we will now proceed to show that every base b with $|b| \geq 4$ has *infinitely many* good digit sets with and without zero — see Corollaries 3.8 and 3.15. This was already shown for digit sets with zero by B. Kovács and A. Pethő [16, Section 4] for negative b , and by D. Matula [15] for any integer b (both taking $|b| \geq 3$). We will generalise their methods to our case.

Lemmas 2.16 and 2.17 tell us that at least one nonzero digit in the set must be small. The approach of Kovács and Pethő is to start from the standard digits $\{0, 1, \dots, |b| - 1\}$ and replace just one digit by a much larger number. We will adapt their proof to start from any good digit set such that $|d| \leq |b|$ for all digits d , and use this to show that for any integer base b with $|b| \geq 4$ there exist infinitely many digit sets \mathcal{D} , both with and without zero, such that $(\mathbb{Z}, b, \mathcal{D})$ is a number system. The case $|b| = 3$ unfortunately remains open, as our methods do not work for it. For the special case $b = -2$ we will characterise *all* valid digit sets later (see Theorem 4.1 below).

Definition 3.1 *Let $(\mathbb{Z}, b, \mathcal{D})$ be a pre-number system. If $a = \sum_{i=0}^{\ell} d_i b^i$ for some digits $d_i \in \mathcal{D}$, we say that a has length $\ell + 1$, and write $L(a) = \ell + 1$. Assume $a \neq 0$. If the expansion for a is minimal, and therefore unique, we call d_{ℓ} the most significant digit of a , and write $\text{MSD}(a)$.*

Note that we have $\text{MSD}(a) \neq 0$ by the minimality assumption.

Besides the functions $L(a)$ and $\text{MSD}(a)$, we will use the following notation. We let $(\mathbb{Z}, b, \mathcal{D})$ be a number system, such that $|d| \leq |b|$ for all $d \in \mathcal{D}$. We fix some $u \in \mathbb{Z}$ with $1 \leq |u| \leq |b| - 1$, some integer $k \geq 1$, and one digit $d \in \mathcal{D}$, which is not the zero digit. Then, let $\tilde{d} = d - ub^k$, and $\tilde{\mathcal{D}} = \mathcal{D} \setminus \{d\} \cup \{\tilde{d}\}$. We write \mathcal{A} and $\tilde{\mathcal{A}}$ for the attractors of $(\mathbb{Z}, b, \mathcal{D})$ and $(\mathbb{Z}, b, \tilde{\mathcal{D}})$, respectively.

The case where $b > 0$. We want to derive conditions on u and d that allow us to conclude that $(\mathbb{Z}, b, \tilde{\mathcal{D}})$ is a number system for infinitely many values of k . We start with a sharp lower bound on numbers with a given expansion length. Recall that we assume $|d| \leq b$ for all $d \in \mathcal{D}$.

Lemma 3.2 Assume $b \geq 3$, and let $a = \sum_{i=0}^{\ell} d_i b^i$ be a minimal expansion, with digits in \mathcal{D} . Then a and d_ℓ have the same sign, and:

- (i) if $0 \in \mathcal{D}$, then $|a| \geq \frac{b^\ell + b - 2}{b-1}$;
- (ii) if $0 \notin \mathcal{D}$, then $|a| \geq \frac{b^\ell - 2b^{\ell-1} + b}{b-1}$.

Proof. As $b > 0$, by Theorem 2.13 and the remarks following it, both 1 and -1 are in \mathcal{D} , while neither $b-1$ nor $-b+1$ are in \mathcal{D} . Thus, we have $|d| \leq b-2$ whenever $d \not\equiv 0 \pmod{b}$.

Suppose that $0 \in \mathcal{D}$. Then we know that $|d_i| \leq b-2$ for all i , and therefore

$$\left| \sum_{i=0}^{\ell-1} d_i b^i \right| \leq (b-2) \frac{b^\ell - 1}{b-1} < b^\ell.$$

Furthermore, we have $d_\ell \neq 0$ by the minimality assumption. It follows that

$$|a| \geq b^\ell - (b-2) \frac{b^\ell - 1}{b-1} = \frac{b^\ell + b - 2}{b-1}.$$

If $0 \notin \mathcal{D}$, minimality means that the expansion does not start with the zero expansion $(b, -1)$ or $(-b, 1)$ (depending on whether b or $-b$ is in \mathcal{D}). Thus, either $|d_\ell| > 1$ or $|d_\ell| = 1$ and $|d_{\ell-1}| \leq b-2$. In the first case, $|d_i| \leq b$ for $0 \leq i \leq \ell-1$, so

$$|a| \geq 2b^\ell - b \frac{b^\ell - 1}{b-1} = \frac{b^{\ell+1} - 1}{b-1}.$$

In the second, we have

$$\left| \sum_{i=0}^{\ell-1} d_i b^i \right| \leq (b-2)b^{\ell-1} + b(b^{\ell-2} + \dots + b + 1) = b^\ell - 2b^{\ell-1} + \frac{b^\ell - b}{b-1} < b^\ell,$$

so that

$$|a| \geq b^\ell - \left(b^\ell - 2b^{\ell-1} + \frac{b^\ell - b}{b-1} \right) = \frac{b^\ell - 2b^{\ell-1} + b}{b-1}. \quad \square$$

Lemma 3.3 Assume $b \geq 3$; if $0 \notin \mathcal{D}$, also assume $|u| \leq b-2$. If a is in $\tilde{\mathcal{A}}$, then $L(a) \leq k+1$, and $L(a) = k+1$ implies $|\text{MSD}(a)| = 1$.

Proof. Let $a \in \tilde{\mathcal{A}}$. We may assume that $\tilde{d} = d - ub^k$ has maximum absolute value in $\tilde{\mathcal{D}}$, since otherwise $|\tilde{d}| \leq b$ and we can apply Theorem 2.13 to decide if $\tilde{\mathcal{D}}$ is a valid digit set. Thus by Lemma 2.6, we have $|a| \leq \frac{|u|b^k + |d|}{b-1} \leq \frac{|u|}{b-1}b^k + 1$.

If $0 \in \mathcal{D}$, this bound is simply $|a| \leq b^k + 1 = \frac{b^{k+1} - b^k + b - 1}{b-1}$. Now assume also that $L(a) \geq k+2$; then by Lemma 3.2, we have $|a| \geq \frac{b^{k+1} + b - 2}{b-1}$. This is a contradiction.

If $0 \notin \mathcal{D}$, we assumed $|u| \leq b-2$, so $|a| \leq \frac{b^{k+1} - 2b^k + b - 1}{b-1}$. Assume that $L(a) \geq k+2$; then by Lemma 3.2, we have $|a| \geq \frac{b^{k+1} - 2b^k + b}{b-1}$, which is impossible.

Now assume $L(a) = k + 1$, and $|\text{MSD}(a)| > 1$. Then the lower bounds for $|a|$ given by Lemma 3.2 are $b^k + \frac{b^k + b - 2}{b - 1}$ and $b^k + \frac{b^k - 2b^{k-1} + b}{b - 1}$, respectively, and these are still in contradiction with $|a| \leq \frac{|u|}{b-1}b^k + 1$. \square

Lemma 3.4 *Assume $b \geq 3$. Let $a \in \mathbb{Z}$ have $|a| \leq b - 1$; then $L(a) \leq 2$, and if $L(a) = 2$, then $|\text{MSD}(a)| = 1$.*

Proof. This follows directly from Lemma 3.2: if we assume $L(a) = 3$, we find $|a| \geq b$, a contradiction, and the same happens if we assume $L(a) = 2$ and $|\text{MSD}(a)| \geq 2$. \square

Definition 3.5 *Assume $b \geq 3$. Recall our fixed digit $d \in \mathcal{D}$. For an integer $k \geq 0$, define*

$$\begin{aligned} D_k &= \{(d_0, d_1, \dots, d_k) : d_i \in \mathcal{D} \text{ for } 0 \leq i \leq k-1, d_k \in \{-1, 0, 1\}\}, \\ \tilde{D}_k &= \{(d_0, d_1, \dots, d_k) \in D_k : d_i \neq d \text{ for } 0 \leq i \leq k\}. \end{aligned}$$

Clearly, D_k contains all digit expansions with digits in \mathcal{D} and length padded to exactly $k + 1$, such that the most significant digit is at most 1 in absolute value. If $0 \notin \mathcal{D}$, we still allow $d_k = 0$, because otherwise it is not always possible to pad exactly to the required length. The subset \tilde{D}_k consists of all elements of D_k that have no components equal to d .

Next, we define the function $\Phi_k : D_k \rightarrow D_k$ as follows. Let $\mathbf{d} = (d_0, \dots, d_k) \in D_k$. If $d_0 = d$, our fixed digit, then

$$\Phi_k(\mathbf{d}) = (d_1, \dots, d_{k-1}, d'_0, d'_1) \tag{3.1a}$$

where d'_0 and d'_1 in \mathcal{D} are such that $d'_0 + d'_1 b = d_k + u$. This is possible by Lemma 3.4. If $d_0 \neq d$, then

$$\Phi_k(\mathbf{d}) = \begin{cases} (d_1, \dots, d_k, 0) & \text{if } d_k \neq 0 \text{ or } 0 \in \mathcal{D} \\ (d_1, \dots, d_{k-1}, d'_0, d'_1) & \text{otherwise,} \end{cases} \tag{3.1b}$$

where d'_0 and d'_1 in \mathcal{D} satisfy $d'_0 + d'_1 b = 0$.

Lemma 3.6 *Assume $b \geq 3$; if $0 \notin \mathcal{D}$, also assume $|u| \leq b - 2$. Then Φ_k is well defined. Furthermore, if for each $\mathbf{d} \in D_k$ there exists an $n \geq 0$ such that $\Phi_k^n(\mathbf{d}) \in \tilde{D}_k$, then $(\mathbb{Z}, b, \tilde{\mathcal{D}})$ is a number system.*

Proof. We extend an argument that was already used in [16,15]. It runs as follows. In order to prove that $(\mathbb{Z}, b, \tilde{\mathcal{D}})$ is a number system, it suffices that every element in the attractor $\tilde{\mathcal{A}}$ has a finite expansion with digits in $\tilde{\mathcal{D}}$. Let

$a \in \tilde{\mathcal{A}}$ and let $a = \sum_{i=0}^k d_i b^i$ be its expansion with digits in \mathcal{D} , padded to length $k+1$; if necessary, we may take $d_k = 0$, even if $0 \notin \mathcal{D}$. It follows that $\mathbf{d} = (d_0, \dots, d_k)$ is in D_k .

There are two cases. If $d_0 \neq d$, then a has a finite expansion with digits in $\tilde{\mathcal{D}}$ if and only if $(a - d_0)/b$ has such an expansion. If $d_0 = d$, we replace d_0 by $d - ub^k$; to make up, we also replace d_k by $d_k + u$. Then a has an expansion of the desired form if and only if $(a - (d - ub^k))/b$ does.

We claim that if $\mathbf{d} \in D_k$ is an expansion of a , then $\Phi_k(\mathbf{d})$ is an expansion of $(a - d_0)/b$ and $(a - (d - ub^k))/b$, in the respective cases. Clearly, if this claim holds, then the lemma follows by induction, because the expansions in \tilde{D}_k are of the desired form.

We prove the claim, using the same two cases. Let $\mathbf{d} \in D_k$ be an expansion of a , with $d_0 \neq d$; then we get an expansion of $(a - d_0)/b$ by deleting d_0 and shifting the other digits down. To have an expansion of length $k+1$ again, we can add a digit 0 if $0 \in \mathcal{D}$. If $0 \notin \mathcal{D}$, we must be careful. If $d_k = 0$ already, by adding 0 we would get two zeros in succession, and this is not allowed by the definition of D_k . Instead, we also delete d_k , and add the zero expansion of $(\mathbb{Z}, b, \mathcal{D})$, which is either $(b, -1)$ or $(-b, 1)$. If $d_k \neq 0$, however, we cannot do this, and we add a 0. This corresponds to the definition (3.1b) of $\Phi_k(\mathbf{d})$ in this case.

If $d_0 = d$, as already said, we replaced d_0 by $d - ub^k$, and d_k by $d_k + u$. Now consider $(a - (d - ub^k))/b$. As before, we delete $d - ub^k$ and shift the other digits down. Of course, $d_k + u$ need not be a digit. However, because $d_k \in \{-1, 0, 1\}$ and $|u| \leq b-1$ or $b-2$, according as $0 \in \mathcal{D}$ or not, $d_k + u$ can be written $d'_0 + d'_1 b$ with $d'_0 \in \mathcal{D}$ and $d'_1 \in \{-1, 0, 1\}$, by Lemma 3.4. Therefore, we replace $d_k + u$ by this expansion of length 1 or 2, adding a 0 if necessary. This gives us an expansion of length $k+1$ that satisfies the definition of D_k , and corresponds to the definition of $\Phi_k(\mathbf{d})$ in (3.1a). The claim is proved. \square

The next result generalises Theorem 5 in [16].

Theorem 3.7 *Let $(\mathbb{Z}, b, \mathcal{D})$ be a number system, where $b \geq 3$ and where $|d| \leq b$ for all $d \in \mathcal{D}$. Fix some $d \in \mathcal{D}$ and some integer u with $|u| \leq b-1$; if $0 \notin \mathcal{D}$, assume $|u| \leq b-2$. Let \mathcal{B} be the set of digits in \mathcal{D} that occur in the expansions of $0, u+1, u$, and $u-1$. If $d \notin \mathcal{B}$, then we may replace d in \mathcal{D} by $\tilde{d} = d - ub^k$, for any $k \geq 1$, without affecting the number system property.*

Proof. Let $\mathbf{d} \in D_k$, as defined above; by Lemma 3.6, it is enough to show that $\Phi_k(\mathbf{d}) \in \tilde{D}_k$ for n large enough. Now whatever the components of \mathbf{d} are, they are gradually replaced by the components introduced at the end by the

repeated application of Φ_k . These new components are digits that occur in the expansion of 0, of $1 + u$, of u , and of $-1 + u$. Thus if d is distinct from all these digits, then for n large enough, $\Phi_k(\mathbf{d})$ will have no components equal to d , as desired. \square

Remarks. The least significant digits of 0, u , $u+1$, and $u-1$, and the possible most significant digits 1 and -1 , together make up the set \mathcal{B} . Therefore, \mathcal{B} has at most 6 elements.

It follows from the proof that the zero digit, being the least significant digit of 0, is always one of the bad digits, and in fact the conclusion of the Theorem is often false if d is congruent to 0 modulo b . For example, although $\mathcal{D} = \{-5, 1, 2, 3, -1\}$ gives a number system with base $b = 5$, the sets $\{-5 + 5^k, 1, 2, 3, -1\}$ for $k \geq 2$ give a cycle $(5 - 5^k)/4 \rightarrow (5 - 5^k)/4$, and the attractors of $\{-5 - 5^k, 1, 2, 3, -1\}$ for $k \geq 2$ do not contain 0.

Examples. Let us apply Theorem 3.7 to some of the starting digit sets that we found in the previous section.

First, let us note that Theorem 3.7 cannot be applied if $b = 3$. Indeed, because u , $u + 1$, and $u - 1$ are incongruent modulo b , we see that \mathcal{B} must contain at least 3 elements. If now $b = 3$, we have no choices left for d .

In fact, we have been unable to find any infinite sequence of valid nonzero digit sets for $b = 3$. However, the set $\{0, 1, 2 - 3^k\}$ was found to be valid for all $k \geq 1$ by Matula [15, Theorem 8]. He used a refinement of our argument for the case where \mathcal{D} has only nonnegative digits, which allows him to start from the digit set $\{0, 1, 2\}$. Of course, with this digit set only nonnegative integers can be represented, but using Theorem 2.9 one can prove that the attractor $\tilde{\mathcal{A}}$ contains only nonnegative elements if we choose u positive. Unfortunately, this argument does not work in the case the starting digit set contains b instead of 0.

Due to these technical problems with $b = 3$, we assume $b \geq 4$ in what follows.

Consider $\mathcal{D} = \{-1, 0, 1, \dots, b - 2\}$; this is a valid digit set by Theorem 2.13. Taking $u = 1$, we find the expansions $0 = (0)$, $u = (1)$, $u + 1 = (2)$, and $u - 1 = (0)$. It follows that $\mathcal{B} = \{0, 1, 2\}$, so we can take $d = -1$ or $d = 3, 4, \dots, b - 2$ and replace it by $\tilde{d} = d - b^k$ for any $k \geq 1$. If we take $u = -1$, the expansion for $u - 1$ becomes $-2 = (b - 2, -1)$, and we obtain $\mathcal{B} = \{-1, 0, b - 2\}$.

For an example without the digit 0, consider $\mathcal{D} = \{-1, 1, 2, \dots, b - 2, b\}$. Again by Theorem 2.13, this digit set is valid. Taking $u = 1$, we expand

$0 = u - 1 = (b, -1)$, $u = (1)$, and $u + 1 = (2)$, so that $\mathcal{B} = \{-1, 1, 2, b\}$. For $u = -1$, we get $\mathcal{B} = \{-1, b - 2, b\}$.

We thus obtain the following basic result.

Corollary 3.8 *For each integer base $b \geq 4$ there exist infinitely many valid digit sets \mathcal{D} containing 0, and infinitely many valid digit sets without 0.*

Proof. For any $k \geq 1$, one can take $\{0, 1, \dots, b - 2\} \cup \{-1 - b^k\}$ and $\{-1, 2, 3, \dots, b - 2, b\} \cup \{1 + b^k\}$, respectively. \square

As another example, let b be odd, and consider the odd digit set \mathcal{D}_{odd} (Definition 2.14). Let us choose $u = 1$; we find the expansions $0 = (b, -1)$, $u = (1)$, $u - 1 = (b, -1)$, and $u + 1 = (-b + 2, 1)$. Consequently, the bad set \mathcal{B} is $\{1, -1, b, -b + 2\}$. For $u = -1$, we have $u + 1 = (b - 2, -1)$, and $\mathcal{B} = \{-1, b - 2, b\}$.

The case where $b < 0$. We now change to the case where the base b is negative, still assuming that we start from a digit set \mathcal{D} with all digits at most equal to $|b|$ in absolute value. Obtaining upper bounds on the expansion length is trickier here than before, because of the sign alternation in powers of b in consecutive terms of the expansion. The results are as follows. Note that we exclude $b = -2$; for this very special case, we refer to Section 4 below.

Lemma 3.9 *Assume $b \leq -3$, and let $a = \sum_{i=0}^{\ell} d_i b^i$ be a minimal expansion, with $d_i \in \mathcal{D}$. Let $L(0)$ be the length of the zero expansion with digits in \mathcal{D} . Then a and $d_{\ell} b^{\ell}$ have the same sign, and, putting $B = |b|$, we have:*

- (i) if $L(0) = 1$ and $\ell \geq 0$, then $|a| \geq \begin{cases} 1 + \frac{B^{\ell}-1}{B^2-1} & \text{if } \ell \text{ is even;} \\ 1 + \frac{B^{\ell}-B}{B^2-1} & \text{if } \ell \text{ is odd.} \end{cases}$
- (ii) if $L(0) = 2$ and $\ell \geq 1$, then $|a| \geq \begin{cases} 1 + \frac{B^{\ell}-B^{\ell-1}+B-1}{B^2-1} & \text{if } \ell \text{ is even;} \\ 1 + \frac{B^{\ell}-B^{\ell-1}-B+1}{B^2-1} & \text{if } \ell \text{ is odd.} \end{cases}$
- (iii) if $L(0) = 3$ and $\ell \geq 2$, then $|a| \geq \begin{cases} 1 + \frac{B^{\ell}-2B^{\ell-2}+1}{B^2-1} & \text{if } \ell \text{ is even;} \\ 1 + \frac{B^{\ell}-2B^{\ell-2}+B}{B^2-1} & \text{if } \ell \text{ is odd.} \end{cases}$

Proof. We write $B = |b|$ throughout. As in the proof of Lemma 3.2, we will show that $|\sum_{i=0}^{\ell-1} d_i b^i|$ is less than B^{ℓ} for minimal expansions. Thus, all claims will follow from the fact that

$$|a| \geq B^{\ell} - |\sum_{i=0}^{\ell-1} d_i b^i|.$$

Now minimising $|a|$ amounts to maximising the second term on the right. This can be done by maximising all d_i with odd i , and minimising those with even i , or conversely.

First, assume $0 \in \mathcal{D}$; this implies $|d| \leq B - 1$ for all $d \in \mathcal{D}$. Because \mathcal{D} is a valid digit set, either 1 or -1 is in \mathcal{D} ; let us assume the former. Thus the expansion with smallest absolute value is given by

$$(\dots, b+2, -b-1, b+2, -b-1, 1).$$

This is explained as follows: we take the most significant digit as small as possible, but cannot make it 0 in a minimal expansion. Then we maximise the second digit, using something positive to get the sign right; we cannot get beyond $-b-1$. Then, we would like to take $b+1$ in the third digit, being maximally negative; but $b+1$ and 1 cannot be in the same digit set. Thus, the third digit is $b+2$ or greater. We find that $\left| \sum_{i=0}^{\ell-1} d_i b^i \right|$ is bounded by

$$(B-1)(B+B^3+\dots+B^{\ell-1}) + (B-2)(1+B^2+\dots+B^{\ell-2}) = B^\ell - 1 - \frac{B^\ell-1}{B^2-1}$$

when ℓ is even, and by

$$B^\ell - 1 - \frac{B^\ell-B}{B^2-1}$$

when ℓ is odd.

Next, assume we have a zero expansion of length 2, which will be either $(-b, 1)$ or $(b, -1)$. Let us assume the former. Minimality now forbids to have $d_\ell = 1$ and $d_{\ell-1} = -b$, so we may assume $d_\ell = 1$ and $d_{\ell-1} = -b-1$. Thus 1, $-b$, and $-b-1$ are in \mathcal{D} , and we see that $b+1 \notin \mathcal{D}$. Therefore, the smallest expansion is given by

$$(\dots, -b, b+2, -b, b+2, -b-1, 1).$$

We find that $\left| \sum_{i=0}^{\ell-1} d_i b^i \right| \leq B^\ell - 1 - \begin{cases} \frac{B^\ell-B^{\ell-1}+B-1}{B^2-1} & \text{if } \ell \text{ is even;} \\ \frac{B^\ell-B^{\ell-1}-B+1}{B^2-1} & \text{if } \ell \text{ is odd.} \end{cases}$

Finally, assume the zero expansion is $(b, -b-1, 1)$ or $(-b, b+1, -1)$; let us say, the former. It follows that -1 and $b+1$ are not in \mathcal{D} , and the smallest expansion is given by

$$(\dots, b, -b-1, b, -b-1, b+2, -b-1, 1).$$

We find that $\left| \sum_{i=0}^{\ell-1} d_i b^i \right| \leq B^\ell - 1 - \begin{cases} \frac{B^\ell-2B^{\ell-2}+1}{B^2-1} & \text{if } \ell \text{ is even;} \\ \frac{B^\ell-2B^{\ell-2}+B}{B^2-1} & \text{if } \ell \text{ is odd.} \end{cases} \quad \square$

Lemma 3.10 *Assume $b \leq -3$, and write $B = |b|$; if $0 \notin \mathcal{D}$, assume $|u| \leq B - 2$. If a is in $\tilde{\mathcal{A}}$, then $L(a) \leq k + 2$, and $L(a) > k$ implies that $|a - \sum_{i=0}^{k-1} d_i b^i| = B^k$.*

Proof. We write $B = |b|$ and let $a \in \tilde{\mathcal{A}}$. The method is the same as for Lemma 3.3, and we will leave the details to the reader. The fact that a is in \mathcal{A} leads to upper bounds on $|a|$, while lower bounds on $|a|$ are provided by Lemma 3.9.

The implication when $L(a) > k$ is proved as follows. If the implication is false, then the lower bounds from Lemma 3.9 for $\ell = k$ or $\ell = k + 1$ can be increased by B^k , and this makes them larger than the upper bound for $|a|$. \square

Lemma 3.11 *Assume $b \leq -3$, and write $B = |b|$. Let $a \in \mathbb{Z}$ with $|a| \leq B - 1$; then $L(a) \leq 3$, and if $L(a) > 1$, then $|a - d_0| = B$.*

Proof. This follows directly from Lemma 3.9: if we assume $L(a) = 4$, we find $|a| \geq B$, a contradiction, and the same happens if we assume $L(a) = 2$ or $L(a) = 3$ and $|a - d_0| \geq 2B$. \square

We now define a discrete dynamical system analogous to the one defined above; see Definition 3.5.

Definition 3.12 *Assume $b \leq -3$. Recall our fixed digit $d \in \mathcal{D}$. For an integer $k \geq 0$, define*

$$\begin{aligned} S &= \{(d_0, d_1) : d_0, d_1 \in \mathcal{D} \cup \{0\}, d_0 + b d_1 \in \{-1, 0, 1\}, \\ &\quad (d_0, d_1) \neq (0, 0) \text{ if } L(0) = 2\}; \\ E_k &= \{(d_0, d_1, \dots, d_{k+1}) : d_i \in \mathcal{D} \text{ for } 0 \leq i \leq k - 1, (d_k, d_{k+1}) \in S\}; \\ \tilde{E}_k &= \{(d_0, d_1, \dots, d_{k+1}) \in E_k : d_i \neq d \text{ for } 0 \leq i \leq k + 1\}. \end{aligned}$$

The set E_k contains all expansions over \mathcal{D} of length $k + 1$ such that the most significant part $d_k + b d_{k+1}$ has absolute value at most 1. The possible pairs (d_k, d_{k+1}) that satisfy this condition depend on \mathcal{D} , and are collected in the set S . In order to get a length of exactly $k + 1$, we allow some digits to be 0, even if 0 is not in \mathcal{D} , just as in the case $b > 0$ (Definition 3.5). Our definition implies that S has 3 elements for every \mathcal{D} , namely the expansions of -1 , 1 , and 0 .

Next, we define the function $\Psi_k : E_k \rightarrow E_k$ as follows. Let $\mathbf{d} = (d_0, \dots, d_{k+1}) \in D_k$. If $d_0 = d$, our fixed digit, then

$$\Psi_k(\mathbf{d}) = (d_1, \dots, d_{k-1}, d'_0, d'_1, d'_2) \quad (3.2a)$$

where d'_0, d'_1, d'_2 in \mathcal{D} are such that $d'_0 + d'_1 b + d'_2 b^2 = d_k + d_{k+1} b + u$. This is possible by Lemma 3.11. Suppose $d_0 \neq d$. If $d_{k+1} \neq 0$ or $0 \in \mathcal{D}$, then

$$\Psi_k(\mathbf{d}) = (d_1, \dots, d_{k+1}, 0). \quad (3.2b)$$

If $d_{k+1} = 0$ and (d'_0, d'_1) is the zero expansion, then

$$\Psi_k(\mathbf{d}) = (d_1, \dots, d_k, d'_0, d'_1). \quad (3.2c)$$

If $d_k = d_{k+1} = 0$ and (d'_0, d'_1, d'_2) is the zero expansion, then

$$\Psi_k(\mathbf{d}) = (d_1, \dots, d_{k-1}, d'_0, d'_1, d'_2). \quad (3.2d)$$

Lemma 3.13 *Assume $b \leq -3$, and write $B = |b|$; if $0 \notin \mathcal{D}$, also assume $|u| \leq B - 2$. Then Ψ_k is well defined. Furthermore, if for each $\mathbf{d} \in E_k$ there exists an $n \geq 0$ such that $\Psi_k^n(\mathbf{d}) \in \tilde{E}_k$, then $(\mathbb{Z}, b, \tilde{\mathcal{D}})$ is a number system.*

Proof. The fact that Ψ_k is well defined, i.e., defines a map from E_k into E_k , follows directly from Lemma 3.10. The rest of the argument is the same as for Lemma 3.6. One uses Lemma 3.11 to show that $d_k + d_{k+1}b + u$ always has an expansion of length at most 3, so that $\Psi_k(\mathbf{d})$ always “fits” into the set E_k . \square

Theorem 3.14 *Let $(\mathbb{Z}, b, \mathcal{D})$ be a number system, where $b \leq -3$, and where $|d| \leq B$ for all $d \in \mathcal{D}$, with $B = |b|$. Fix some $d \in \mathcal{D}$ and some integer u with $|u| \leq B - 1$; if $0 \notin \mathcal{D}$, assume $|u| \leq B - 2$. Let \mathcal{B} be the set of digits in \mathcal{D} that occur in the expansions of 0, $u + 1$, u , and $u - 1$. If $d \notin \mathcal{B}$, then we may replace d in \mathcal{D} by $\tilde{d} = d - ub^k$, for any $k \geq 1$, without affecting the number system property.*

Proof. Let $\mathbf{d} \in E_k$, as defined above; by Lemma 3.6, it is enough to show that $\Psi_k(\mathbf{d}) \in \tilde{E}_k$ for n large enough. Now whatever the components of \mathbf{d} are, they are gradually replaced by the components introduced at the end by the repeated application of Ψ_k . These new components are the digits that occur in the expansion of 0, of $1 + u$, of u , and of $-1 + u$. Thus if d is distinct from all these digits, then for n large enough, $\Psi_k^n(\mathbf{d})$ will have no components equal to d , as desired. \square

Remarks. The same remarks as with Theorem 3.7 apply here. The expansions of 0 , $u + 1$, u , and $u - 1$ among them have at most 4 distinct least significant digits; the more significant digits d_1 and maybe d_2 are all taken from $\{1, -1, -b - 1, b + 1\}$. Therefore, $|\mathcal{B}| \leq 8$.

An example where the conclusion of the Theorem is false when $d \equiv 0 \pmod{b}$ is the following. Although $\mathcal{D} = \{-5, 1, 2, 3, 4\}$ gives a number system with base $b = -5$, the set $\{-5 - (-5)^k, 1, 2, 3, 4\}$ is not valid for $k \geq 2$: we have $-5 - (-5)^k = -5(1 - (-5)^{k-1})$, which is divisible by $1 - (-5) = 6$ for $k \geq 1$, and thus gives a nonzero 1-cycle $\frac{-5 - (-5)^k}{6} \rightarrow \frac{-5 - (-5)^k}{6}$ by Lemma 2.4 if $k \geq 2$.

Examples. Let $b < 0$. For the reasons explained after Theorem 3.7, we cannot apply Theorem 3.14 when $b = -3$. Thus, assume $b \leq -4$. We write $B = |b|$.

Consider the classical digit set $\{0, 1, \dots, B - 1\}$, and take $u = 1$. It is clear that the bad set \mathcal{B} is $\{0, 1, 2\}$, so we may replace d by $d - b^k$ for any $k \geq 1$, if $3 \geq d \geq B - 1$. Now take $u = -1$. We find $u = (B - 1, 1)$ and $u - 1 = (B - 2, 1)$, so that $\mathcal{B} = \{0, 1, B - 2, B - 1\}$. Thus, any d outside the latter set may be replaced by $d + b^k$, for any $k \geq 1$.

Now as an example of a nonzero digit set, let $\mathcal{D} = \{1, 2, \dots, B\}$. We find $0 = (B, 1)$, as $B = -b$, and with $u = 1$, we have $u = (1)$, $u - 1 = (B, 1)$, and $u + 1 = (2)$. Thus $\mathcal{B} = \{1, 2, B\}$. For $u = -1$, we find $u = (B - 1, 1)$, $u - 1 = (B - 2, 1)$, and $u + 1 = (B, 1)$, so that $\mathcal{B} = \{1, B - 2, B - 1, B\}$.

Corollary 3.15 *For each integer base $b \leq -4$ there exist infinitely many valid digit sets \mathcal{D} containing 0, and infinitely many valid digit sets without 0.*

Proof. For any $k \geq 1$, one can take $\{0, 1, \dots, B - 2\} \cup \{B - 1 - b^k\}$ and $\{1, 2, 4, 5, \dots, B\} \cup \{3 - b^k\}$, respectively. \square

With the odd digits \mathcal{D}_{odd} (Definition 2.14), we have $0 = (b, -1)$. For $u = 1$, we get $u + 1 = (b + 2, -1)$, so that $\mathcal{B} = \{-1, 1, b + 2, b\}$. For the more exotic $u = -3$, we get $u = (-3)$, $u - 1 = (B - 4, 1)$, and $u + 1 = (B - 2, 1)$, so that $\mathcal{B} = \{1, -1, -3, B - 4, B - 2\}$.

Finally, as an example of a digit set with a zero expansion of length 3, let $\mathcal{D} = \{b, 1, 2, \dots, B - 1\}$ and $u = 1$. This gives $0 = (b, B - 1, 1)$, and $\mathcal{B} = \{1, 2, B - 1, b\}$.

It is an interesting question whether there also exist infinitely “zero digits” complementing a given digit set. For example, for $b \leq -2$, are there infinitely many multiples cb of b such that $\{cb, 1, 2, \dots, |b| - 1\}$ is a good digit set? As yet, we only have some partial answer to this question. Namely, Theorem 2.12 shows that as $|c| \rightarrow \infty$, with the other digits staying the same, also the length of the zero cycle increases without bound. This contrasts with the infinite families that we gave in this section, where the length of the zero cycle is the same throughout the family.

4 Base -2

The case where the base b of the number system is -2 is special, as several of the general results obtained above do not apply to this case. Examples are Theorem 2.13 about smallest digit sets, Theorem 2.18 that says that only finitely many translates of a given digit set can yield number systems, and the Theorems given in the last section that prove the existence of infinitely many good digit sets.

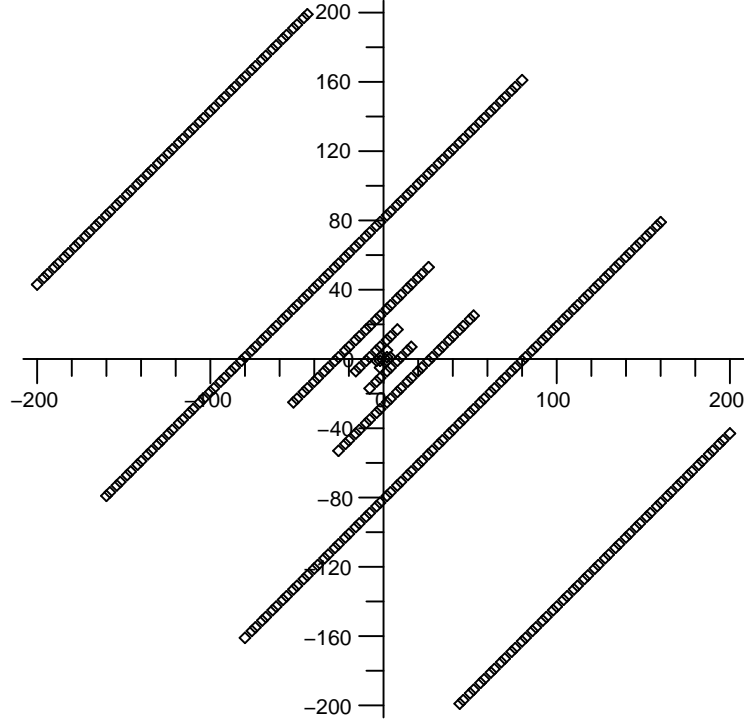
However, in the case of the integers \mathbb{Z} , we have succeeded in determining *all* possible digit sets for the base $b = -2$. It will follow from this characterisation that there are infinitely many good digit sets for this base and that unbounded translation only yields finitely many good such sets. A remarkable feature of this case is that there exist no infinite families of good digit sets obtained by translating one digit by a power of -2 , as in the last section; instead, one can shift by powers of 3.

Theorem 4.1 *Let $d, D \in \mathbb{Z}$, with $d < D$. Then $(\mathbb{Z}, -2, \{d, D\})$ is a number system if and only if*

- (i) *one of $\{d, D\}$ is even and one is odd;*
- (ii) *neither d nor D is divisible by 3, except that the even digit can be 0;*
- (iii) *we have $2d \leq D$ and $2D \geq d$;*
- (iv) *$D - d = 3^i$ for some $i \geq 0$.*

As an example, the Theorem implies that a valid digit set for base -2 that contains 0 must be either $\{0, 1\}$ or $\{0, -1\}$. On the other hand, it follows easily that there are infinitely many valid digit sets without 0, for example the sets $\{1, 3^i + 1\}$ for $i \geq 0$ already discussed earlier.

The figure presents all valid digit sets $\{d, D\}$ for base $b = -2$ with $-200 \leq d < D \leq 200$. As stipulated by condition (iii) of the Theorem, all pairs lie in one of the two obtusely angled regions bounded by $y = 2x$ and $y = \frac{1}{2}x$.



For the proof of the Theorem we present a series of Lemmas. The first result shows that the attractors for base -2 have an especially simple structure: they are always *intervals* in \mathbb{Z} .

Lemma 4.2 *Let $(\mathbb{Z}, -2, \{d, D\})$ be a pre-number system, with attractor \mathcal{A} , and suppose $d < D$. Then*

$$\mathcal{A} = \left\{ \left\lceil \frac{2d-D}{3} \right\rceil, \dots, \left\lfloor \frac{2D-d}{3} \right\rfloor \right\}.$$

Proof. Theorem 2.9 tells us that $\frac{2d-D}{3} \leq a \leq \frac{2D-d}{3}$ for any $a \in \mathcal{A}$. We will show that these bounds are sharp. We use the following argument: on an arithmetic progression of difference 2, the dynamic mapping T is an affine linear map with slope $-\frac{1}{2}$, so such a progression will be mapped, with its order reversed, onto an *interval*. Thus the image of any interval S under T can be computed by splitting S into its even and odd parts (which are $S \cap 2\mathbb{Z}$ and $S \cap (2\mathbb{Z} + 1)$, respectively), and considering the effect of T on these parts separately.

Suppose first that $d + D \equiv 0 \pmod{3}$; then $2d - D$ and $2D - d$ are divisible by 3. Let $a = \frac{2d-D}{3}$ and $A = \frac{2D-d}{3}$; we will prove that $\mathcal{A} = \{a, \dots, A\}$. Note

that $a \equiv D \pmod{2}$ and $A \equiv d \pmod{2}$. We compute

$$\begin{aligned} T(a) &= \frac{\frac{2d-D}{3} - D}{-2} = \frac{2D-d}{3} = A; \\ T(a+1) &= \frac{\frac{2d-D+3}{3} - d}{-2} = \frac{D+d-3}{6}; \\ T(A) &= \frac{\frac{2D-d}{3} - d}{-2} = \frac{2d-D}{3} = a; \\ T(A-1) &= \frac{\frac{2D-d-3}{3} - D}{-2} = \frac{D+d+3}{6} = T(a+1) + 1. \end{aligned}$$

It follows that the arithmetic progression $a, a+2, \dots, A-1$ is mapped to the interval $A, A-1, \dots, T(a+1)+1$, while the other progression $a+1, a+3, \dots, A$ is mapped to $T(a+1), T(a+1)-1, \dots, a$. Thus the interval $\{a, \dots, A\}$ is equal to its image under T , which shows that it is equal to the attractor \mathcal{A} .

Suppose that $d+D \equiv 1 \pmod{3}$. Let us write $a = \lceil \frac{2d-D}{3} \rceil = \frac{2d-D+1}{3}$ and $A = \lfloor \frac{2D-d}{3} \rfloor = \frac{2D-d-2}{3}$; we will prove that $\mathcal{A} = \{a, \dots, A\}$. Note that $a \equiv D+1 \equiv d \pmod{2}$, and that $A \equiv d-2 \equiv d \pmod{2}$. Using this, we compute

$$\begin{aligned} T(a) &= \frac{\frac{2d-D+1}{3} - d}{-2} = \frac{D+d-1}{6}; \\ T(a+1) &= \frac{\frac{2d-D+4}{3} - D}{-2} = \frac{2D-d-2}{3} = A; \\ T(A) &= \frac{\frac{2D-d-2}{3} - d}{-2} = \frac{2d-D+1}{3} = a; \\ T(A-1) &= \frac{\frac{2D-d-5}{3} - D}{-2} = \frac{D+d+5}{6} = T(a) + 1. \end{aligned}$$

We again use the fact that T is affine linear, with slope $-\frac{1}{2}$, on arithmetic progressions of difference 2. Thus, the progression $a, a+2, \dots, A-2, A$ is mapped by T to the interval $a, \dots, T(a)$ (in reversed order), while the progression $a+1, a+3, \dots, A-1$ is mapped to $T(a)+1, T(a)+2, \dots, A$. We see that $\{a, \dots, A\}$ is mapped unto itself by T , which proves the claim.

Finally, the case where $d+D \equiv 2 \pmod{3}$ is reduced to the previous by considering the digits $\{-d, -D\}$. \square

Lemma 4.3 *Let $(\mathbb{Z}, -2, \{d_0, d_1\})$ be a pre-number system, with attractor \mathcal{A} . Write $\delta = d_0 - d_1$. Then $a \in \mathcal{A}$ is contained in a cycle of length ℓ within \mathcal{A} if and only if*

$$(d_0 - 3a) \frac{(-2)^\ell - 1}{-3\delta} = \sum_{i=0}^{\ell-1} \varepsilon_i (-2)^i \quad (4.1)$$

for some $\varepsilon_i \in \{0, 1\}$, and ℓ is minimal with this property.

Proof. For any base b , a cycle of length ℓ in the attractor has the form

$$a_0 \rightarrow a_1 = \frac{a_0 - d_0}{b} \rightarrow a_2 = \frac{\frac{a_0 - d_0}{b} - d_1}{b} = \frac{a_0}{b^2} - \left(\frac{d_0}{b^2} + \frac{d_1}{b} \right) \rightarrow \dots \rightarrow a_\ell = a_0,$$

with $a_i \in \mathcal{A}$ and $d_i \in \mathcal{D}$ for all i . Continuing the expansion of the elements and multiplying through by b^ℓ , we find

$$a_0(1 - b^\ell) = \sum_{i=0}^{\ell-1} d_i b^i.$$

Conversely, it is clear that if $a(1 - b^\ell)$ can be written in this form, for some $a \in \mathcal{A}$, and ℓ is minimal with this property, then a starts a cycle of length ℓ .

In our case, the digits d_i are either d_0 or $d_0 - \delta$. This gives

$$a_0(1 - b^\ell) = d_0 \frac{b^\ell - 1}{b - 1} - \delta \sum_{i=0}^{\ell-1} \varepsilon_i b^i,$$

with $\varepsilon_i \in \{0, 1\}$ for all i . It follows that

$$(d_0 + (b - 1)a_0)(b^\ell - 1) = (b - 1)\delta \sum_{i=0}^{\ell-1} \varepsilon_i b^i.$$

The Lemma now follows by substituting $b = -2$. \square

We will use the q -adic valuation v_q for a prime q : for an integer $b \neq 0$, $v_q(b)$ denotes the exact number of factors q in b .

Lemma 4.4 *Let q be an odd prime, let b be an integer with $|b| \geq 2$, coprime to q , and let n be a nonnegative integer. Then q divides $b^n - 1$ if and only if $\text{ord}_q(b)$ divides n . If q divides $b^n - 1$, then*

$$v_q(b^n - 1) = v_q(n) + v_q(b^{\text{ord}_q(b)} - 1).$$

Proof. This result is a special case of Lucas' *law of repetition*. For a proof, see [19]. \square

Example. Consider the digits $\{30, 111\}$, so $\delta = -81$. The attractor for base -2 with these digits is $\{-17, \dots, 64\}$. Both digits are divisible by 3, which

shows the existence of two 1-cycles. The complete cycle structure is

$$\begin{aligned}\mathcal{A} = & \{10\} \cup \{37\} \cup \{-17, 64\} \cup \{-8, 19, 46\} \cup \{1, 55, 28\} \cup \\ & \{4, 13, 49, 31, 40, -5, 58, -14, 22\} \cup \{-2, 16, 7, 52, -11, 61, 25, 43, 34\} \\ & \{0, 15, 48, -9, 60, -15, 63, 24, 3, 54, -12, 21, 45, 33, 39, 36, -3, 57, 27, 42, \\ & \quad -6, 18, 6, 12, 9, 51, 30\} \cup \\ & \{-1, 56, -13, 62, -16, 23, 44, -7, 59, 26, 2, 14, 8, 11, 50, -10, 20, 5, 53, 29, \\ & \quad 41, 35, 38, -4, 17, 47, 32\}.\end{aligned}$$

Of these, the cycle lengths ℓ that are powers of 3 are not that surprising, because $(-2)^\ell - 1$ is then divisible by ℓ , and the remaining factors of the denominator 3δ are found in $(d_0 - 3a)$. The 2-cycle is legitimised by the following calculation: the factor $(-2)^2 - 1$ cancels the 3 in the denominator, while we have $d_0 - 3 \cdot (-17) = 81$ and $d_0 - 3 \cdot 64 = -162$, both of which are divisible by δ .

Lemma 4.5 *Let $(\mathbb{Z}, -2, \{d_0, d_1\})$ be a pre-number system, with attractor \mathcal{A} . Then \mathcal{A} consists of exactly one cycle if and only if either $|d_0 - d_1| = 1$, or*

- (i) $|d_0 - d_1| = 3^i$ for some $i \geq 1$, and
- (ii) $3 \nmid d_0$ and $3 \nmid d_1$.

Proof. Write $d_1 = d_0 - \delta$ as above, so δ is an odd integer. We first prove the “if”-part.

First, assume $|\delta| = 1$. If $d_0 + d_1 \not\equiv 0 \pmod{3}$, then by Lemma 4.2, \mathcal{A} consists of only one element, and the claim is obvious. If $d_0 + d_1 \equiv 0 \pmod{3}$, then \mathcal{A} has 2 elements, again by Lemma 4.2. If the claim fails, there must be a 1-cycle in \mathcal{A} , and this implies that either d_0 or d_1 is divisible by 3, by Corollary 2.5. But this contradicts the assumption that $d_0 + d_1 \equiv 0 \pmod{3}$. It follows that \mathcal{A} has a single 2-cycle, as desired.

Next, assume $|\delta| = 3^i$ for some $i \geq 1$. As remarked earlier, if 3 divides either d_0 or d_1 , we immediately obtain a 1-cycle in \mathcal{A} . Therefore we exclude this case, and it follows that $d_0 + d_1 \not\equiv 0 \pmod{3}$. By Lemma 4.2, we conclude that

$$|\mathcal{A}| = |\delta| = 3^i.$$

Let ℓ be the length of the longest cycle in \mathcal{A} . By Lemma 4.3, and because $3 \nmid d_0$, we conclude that $3^{i+1} \mid (-2)^\ell - 1$. Now by Lemma 4.4, taking $b = -2$ and $q = 3$, we find that

$$3^{i+1} \mid (-2)^\ell - 1 \Rightarrow 3^i \mid \ell.$$

Because $\ell \leq |\delta|$, it follows that $\ell = |\delta|$, so that \mathcal{A} consists of just one cycle, and the first half of the Lemma is proved.

Now we prove the “only if”-part. Suppose that \mathcal{A} consists of just one cycle. We distinguish two cases, namely whether 3 divides δ or not.

First, assume that 3 divides δ . Now either both d_0 and d_1 are divisible by 3, or neither of them is. If both are divisible by 3, then the attractor has two distinct 1-cycles, which is a contradiction. Thus, 3 divides neither of d_0 and d_1 . By Lemma 4.2, we find that \mathcal{A} is an interval of length $|\delta|$, so that we have just one cycle of length $|\delta|$.

Now consider (4.1). Because \mathcal{A} contains an element from every residue class modulo δ , and because $3 \nmid d_0$, we can choose $a_0 \in \mathcal{A}$ so that $\gcd(d_0 - 3a_0, \delta) = 1$. It follows that

$$3\delta \mid (-2)^{|\delta|} - 1,$$

and this does not hold for any smaller exponent than $|\delta|$. We will show that this implies that $|\delta|$ is a power of 3.

The assumption means that the order of -2 in the multiplicative group $(\mathbb{Z}/3\delta\mathbb{Z})^*$ is equal to $|\delta|$. But this order divides the order of the group, which is $\phi(3|\delta|) = 3\phi(|\delta|)$, as we assume that $3 \mid \delta$. Let p be the largest prime divisor of δ , and suppose $p > 3$. Then $\phi(3|\delta|)$ has less factors p than δ , so that the divisibility relation is impossible. It follows that δ is a power of 3.

Finally, assume that 3 does not divide δ . If 3 divides d_0 , then 3 does not divide d_1 , and \mathcal{A} has exactly one 1-cycle. It follows that \mathcal{A} has just one element. Also, we have $d_0 + d_1 \not\equiv 0 \pmod{3}$, so $|\mathcal{A}| = |\delta|$ by Lemma 4.2. We obtain $|\delta| = 1$, as desired.

If 3 divides neither of d_0 or d_1 , then one easily verifies that $d_0 + d_1 \equiv 0 \pmod{3}$. In this case, Lemma 4.2 shows that $\frac{2D-d}{3}$ and $\frac{2d-D}{3}$ are in \mathcal{A} . But these two elements constitute a 2-cycle under T , and it follows that \mathcal{A} has just these two elements. As $|\mathcal{A}|$ is equal to $|\delta| + 1$, again by Lemma 4.2, we see that $|\delta| = 1$, as desired. \square

Proof of Theorem 4.1 The condition of having one even and one odd digit is obviously necessary. Now the number system condition is equivalent to the requirement that the attractor \mathcal{A} consists of exactly one cycle under the dynamic map T , and that this cycle contains 0.

By Lemma 4.5, the attractor has one cycle if and only if $D - d = 1$, or $D - d = 3^i$ for some $i \geq 1$ and neither D nor d is divisible by 3. Next, Lemma 4.2 tells us whether 0 is in the attractor, as follows.

If $D - d = 1$ and 3 divides one of the digits, we have $D + d \not\equiv 0 \pmod{3}$, so \mathcal{A} consists of just one element. If $3 \mid D$, then this element is $-D/3$, and if $3 \mid d$, it is $-d/3$, as these elements generate 1-cycles. It follows that the digit divisible by 3 must be 0.

If $D - d = 1$ and 3 does not divide a digit, then $D + d \equiv 0 \pmod{3}$, so \mathcal{A} has just the elements $\frac{2d-D}{3}$ and $\frac{2D-d}{3}$, forming a 2-cycle. One of these elements is 0, and one verifies that $2d \leq D$ and $2D \geq d$ are necessary and sufficient conditions for this to hold.

If $D - d = 3^i$ for $i \geq 1$, and 3 does not divide a digit, then $D + d \not\equiv 0 \pmod{3}$. Here again, from the form of \mathcal{A} given by Lemma 4.2, one easily verifies that the two conditions $2d \leq D$ and $2D \geq d$ exactly ensure that $0 \in \mathcal{A}$. \square

Acknowledgements

The research leading to this paper was supported by the Austrian Science Foundation FWF, project S9606, which is part of the Austrian National Research Network “Analytic Combinatorics and Probabilistic Number Theory.”

The anonymous referee is to be thanked for his/her useful suggestions.

References

- [1] V. Grünwald, Intorno all’ aritmetica dei sistemi numerici a base negativa con particolare riguardo al sistema numerico a base negativo-decimale per lo studio delle sue analogie coll’ aritmetica ordinaria (decimale), *Giornale di matematiche di Battaglini* 23 (1885) 203–221.
- [2] C. E. van de Woestijne, Algebraic aspects of integral number systems, in preparation.
- [3] D. E. Knuth, The art of computer programming. Vol. 2: Seminumerical algorithms, 3rd Edition, Addison-Wesley Publishing Co., Reading, Mass., 1998.
- [4] G. Barat, V. Berthé, P. Liardet, J. Thuswaldner, Dynamical directions in numeration, *Ann. Inst. Fourier (Grenoble)* 56 (7) (2006) 1987–2092.
- [5] W. J. Gilbert, Radix representations of quadratic fields, *J. Math. Anal. Appl.* 83 (1) (1981) 264–274.
- [6] C. E. van de Woestijne, Deterministic equation solving over finite fields, Ph.D. thesis, Universiteit Leiden (2006).

- [7] S. Akiyama, C. Frougny, J. Sakarovitch, Powers of rationals modulo 1 and rational base number systems, to appear in Israel J. Math.
- [8] A. M. Odlyzko, Nonnegative digit sets in positional number systems, Proc. London Math. Soc. (3) 37 (2) (1978) 213–229.
- [9] J. C. Lagarias, Y. Wang, Nonnegative radix representations for the orthant \mathbf{R}_+^n , Trans. Amer. Math. Soc. 348 (1) (1996) 99–117.
- [10] S. Akiyama, Positive finiteness of number systems, in: Number theory, Vol. 15 of Dev. Math., Springer, New York, 2006, pp. 1–10.
- [11] G. E. Michalek, Base N just touching covering systems, Publ. Math. Debrecen 58 (4) (2001) 549–557.
- [12] J. A. Muir, D. R. Stinson, Alternative digit sets for nonadjacent representations, SIAM J. Discrete Math. 19 (1) (2005) 165–191 (electronic).
- [13] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, F. Vercauteren (Eds.), Handbook of elliptic and hyperelliptic curve cryptography, Discrete Mathematics and its Applications, Chapman & Hall/CRC, Boca Raton, FL, 2006.
- [14] N. Thériault, SPA resistant left-to-right integer recodings, in: Selected areas in cryptography 2005, Vol. 3897 of Lecture Notes in Comput. Sci., Springer, Berlin, 2006, pp. 345–358.
- [15] D. W. Matula, Basic digit sets for radix representation, J. Assoc. Comput. Mach. 29 (4) (1982) 1131–1143.
- [16] B. Kovács, A. Pethő, Canonical systems in the ring of integers, Publ. Math. Debrecen 30 (1-2) (1983) 39–45.
- [17] S. Akiyama, J. M. Thuswaldner, A survey on topological properties of tiles related to number systems, Geom. Dedicata 109 (2004) 89–105.
- [18] W. Bosma, Signed bits and fast exponentiation, J. Théor. Nombres Bordeaux 13 (1) (2001) 27–41, 21st Journées Arithmétiques (Rome, 1999).
- [19] E. Artin, The orders of the linear groups, Comm. Pure Appl. Math. 8 (1955) 355–365, reprinted in [20], pages 387–397.
- [20] E. Artin, The collected papers of Emil Artin, Edited by Serge Lang and John T. Tate, Addison–Wesley Publishing Co., Inc., Reading, Mass.-London, 1965.